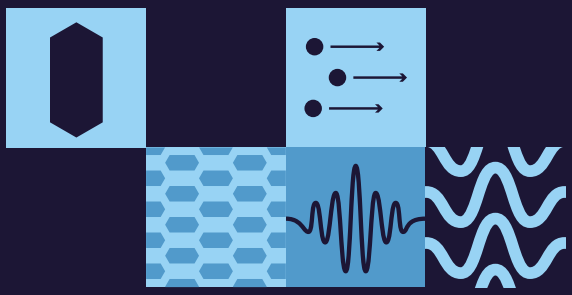
РКЦ | Российский Квантовый Центр



Квантовая криптография

Методическое пособие для World Skills

Аннотация

Квантовая криптография – молодая технология, использующая фундаментальные законы квантовой физики для решения задач защищенной передачи информации. Квантовая криптография зародилась на абстрактных идеях, которыев 70-х годах XX века выдвинул Стефан Визнер и которые получили развитие только через 10 лет. Еще в 90-е годы идеи квантовой информации воспринимались многими физиками как нечто близкое скорее к физическим аспектам философии. В 2000-е задача квантового распределения ключа не только реализована на промышленном уровне, но и пришла в виде учебной дисциплины в ВУЗы.

Оглавление

1. Квантовое распределение ключа.

Используя факт существования неизмеримых одновременно величин (квантовый индетерминизм) и состояние суперпозиции, можно осуществлять закрытую передачу данных [1]. Пусть из пункта А в пункт Б требуется передать конфиденциальные данные. В криптографии этому процессу придают некоторую одушевленность, называя передатчик информации Алисой, а приемник – Бобом. Для шифрования данных нужно чтобы и у Алисы, и у Боба были одинаковые ключи, так чтобы при помощи одного из них можно было бы зашифровать данные, а при помощи другого – расшифровать. Проблема в том, как передать ключ от Алисы к Бобу, или наоборот? Если бы был надежный, защищенный от перехвата, способ передачи ключа (в криптографической терминологии – способ распределения ключа), то и не было бы необходимости шифровать данные, их можно было бы передать тем же способом. В данном случае, ключ – это просто тоже некоторое количество никому не известной, кроме Алисы и Боба, информации.

Будем рассматривать линейную поляризацию фотона в двумерном гильбертовом пространстве: для того, чтобы задать направление поляризации нам нужна ось, чтобы выделить направление в пространстве и п
ривязать к этому базис. Рассмотрение поляризации в вертикально-горизонтальном базисе будем обозначать значком ⊕, в диагональном-антидиагональном – ⊗. Если фотон поляризован вертикально, т.е. находится в состоянии, описываемом вектором $|\updownarrow\rangle$, и мы проводим измерение в базисе ⊗, то вероятность обнаружить фотон в состоянии $|\nearrow\rangle$ будет равна вероятности обнаружить фотон в состоянии $|\nwarrow\rangle$, равна 0,5, Рис. 1. Математически это выражается следующим образом:

$$\begin{aligned} |\updownarrow\rangle &= 1/\sqrt{2}\,|\nearrow\rangle + 1/\sqrt{2}\,|\nwarrow\rangle \\ |\leftrightarrow\rangle &= 1/\sqrt{2}\,|\nearrow\rangle - 1/\sqrt{2}\,|\nwarrow\rangle \end{aligned} \qquad (1)$$

Это означает, что состояние $|\updownarrow\rangle$ состоит из суперпозиции состояний $|\nearrow\rangle$ и $|\nwarrow\rangle$, причем вероятность обнаружить фотон в состоянии $|\nearrow\rangle$ или $|\nwarrow\rangle$ равна квадрату множителя (в данном случае $1/\sqrt{2}$) соответствующего состояния. То же касается и состояния $|\leftrightarrow\rangle$. Здесь знак минус возникает из необходимости некоторого математического согласования, а именно из требования ортогональности, его положение в этой системе уравнений зависит от выбора направления координатных осей в базисах и выбора направления поворота одного базиса относительно другого. В нашем случае это не играет существенной роли.

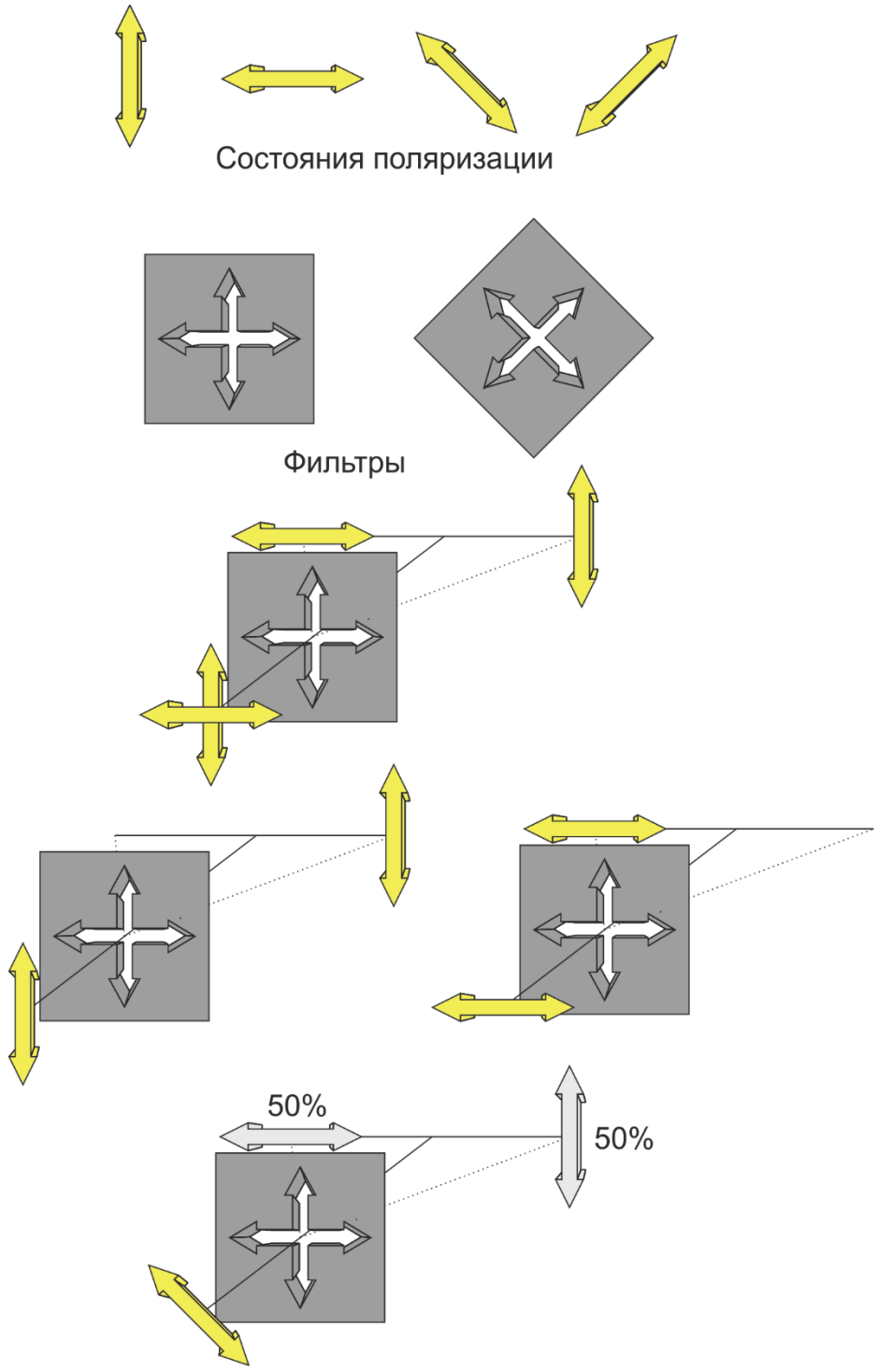


Рис. 1 Измерение поляризации фотонов в различных базисах как пропускание через фильтр.

Если измерить поляризацию фотона в базисе с неопределенной поляризацией, то в этом базисе она станет определенной, а в другом базисе – перестанет быть определенной.

Алиса, посылая Бобу фотон, должна выбрать базис поляризации. Ограничим этот выбор двумя базисами: Алиса может поляризовать фотон в базисе ⊕ (говорят «фотон, приготовленный в базисе ⊕») или в базисе ⊗. Боб не знает в каком базисе фотон был приготовлен, а Алиса выбирает базисы приготовления случайно. Теперь Боб может провести измерения поляризации фотона как в ⊕, так и в ⊗ базисе. Базис измерения Боб тоже выбирает случайно. Если базисы приготовления и измерения поляризации случайно совпадут, то и у Алисы и у Боба будет одинаковая информация о поляризации фотона. Если Боб случайно выберет для измерения другой базис, не тот в котором фотон приготовила Алиса, то результат измерения поляризации будет случайным и не несущим информацию. Договариваемся, что состоянию $|\updownarrow\rangle$ будет соответствовать логическая 1, состоянию $|\leftrightarrow\rangle$ - логический 0, также и для состояний $|\nearrow\rangle$ и $|\nwarrow\searrow\rangle$ – 1 и 0. Таким образом, Алиса пересылает Бобу серию фотонов. Потом они по открытому каналу сверяют базисы и выбрасывают все те измерения, которые были проделаны в базисах, не совпадающих с базисами приготовления. Таким образом, у Алисы и у Боба должны быть одинаковые последовательности битов, при этом они секретные: результаты своих измерений Боб, разумеется, не сообщает. Этот метод бесполезен для передачи информации: Алиса не знает заранее какие биты из последовательности будут выброшены, но он отлично подходит для передачи случайной битовой последовательности, которую можно будет использовать для шифрования данных. Таким образом можно осуществлять квантовое распределение ключа.

Практическая реализация квантового распределения ключа с поляризационным кодированием может быть осуществлена с использованием устройства, которое управляемо поворачивает поляризацию (ячейка Поккельса) и поляризационного светоделителя PBS [2]. При помощи ячейки Поккельса Боб может осуществлять выбор между базисами ⊕ и ⊗, подавая на ячейку соответствующий электрический сигнал. Дальше оптический сигнал разделяется поляризационным светоделителем на две взаимно ортогональных поляризационных составляющих, каждая из которых приходит на свой детектор. Если базис, выбранный Бобом, совпадает с базисом Алисы, то должен сработать детектор, соответствующий поляризации светового импульса, номер детектора определит значение бита полученной информации. Если базис был выбран неправильно, то случайным образом сработает один из детекторов. Конечно, если в импульсе не один фотон, а больше, то может сработать два детектора. Собственно, мы даже можем судить по тому, сколько детекторов сработало, правильно или неправильно мы выбрали базис измерения. Но нам нельзя знать заранее насколько правильно мы выбрали базис, и для этого нам обязательно нужны однофотонные импульсы.

Теперь введем третий персонаж, который будет подслушивать закрытый канал, традиционно это Ева, от английского eavesdropper – подслушивающий. Точно так же, как и Боб, Ева может измерить поляризацию фотона, но также, как и Боб она не знает в каком базисе он был приготовлен. После измерения фотона, Ева пересылает его дальше Бобу (ей же нельзя себя обнаружить). Однако, если она выбирает для измерения не тот базис, в котором фотон приготовила Алиса, то она меняет базис приготовления фотона и, таким образом, в ключ Боба закрадываются ошибки. Правильнее так: количество ошибок в ключе Боба возрастает, потому что когда передача идет на однофотонном уровне, то ошибки возникают неизбежно. У Евы с Бобом базисы различаются – и тот и другой выбирают их случайным образом. Таким образом, у Евы получается меньше полезной информации, чем у Боба. Ключевым моментом здесь является то обстоятельство, что Еву можно обнаружить по возрастанию количества ошибок в ключе Боба. Пожалуй, это и есть самое важное свойство квантовой криптографии – Ева не может скрыть своего присутствия.

Схематично процедуру квантового распределения ключа можно свести к следующей таблице :

Таблица 1

1. Базис Алисы	⊗	⊕	⊕	⊗	⊕	⊗	⊗	⊕	⊗	⊗	⊕
Значение бита Алисы	1	0	1	0	0	1	0	1	1	1	1
Алиса посылает	$\|\nearrow\rangle$	$\|\leftrightarrow\rangle$	$\|\updownarrow\rangle$	$\|\searrow\rangle$	$\|\leftrightarrow\rangle$	$\|\nearrow\rangle$	$\|\searrow\rangle$	$\|\updownarrow\rangle$	$\|\nearrow\rangle$	$\|\nearrow\rangle$	$\|\updownarrow\rangle$
2. Базис Боба	⊗	⊕	⊗	⊕	⊕	⊗	⊗	⊗	⊕	⊕	⊕
Значение бита Боба	1	0	0	0	0	1	0	1	0	1	1
3. Тот же базис?	да	да	нет	нет	да	да	да	нет	нет	нет	Да
У Алисы остается	1	0			0	1	0				1
У Боба остается	1	0			0	1	0				1

1. Алиса случайным образом выбирает базис и поляризацию своих однофотонных импульсов и посылает их Бобу.
2. Для каждого импульса Боб также случайным образом выбирает базис, в котором он измеряет поляризацию импульса. Он либо получает значение бита 0 или 1, либо ничего не регистрирует из-за потерь связи при детектировании. Последовательность всех полученных битов называется сырым ключом.
3. Боб использует открытый канал, чтобы сообщить Алисе номера измерений в которых было срабатывание одного детектора и каком базисе проводились эти измерения. При этом, Боб не сообщает результат измерения. В тех случаях, когда Алиса и Боб использовали один и тот же базис, ⊕ или ⊗, они должны получить одинаковые биты. Последовательность этих битов называется просеянным ключом. При этом, из-за несовершенства

процесса измерения и из-за потенциального подслушивания, возникнет некоторое количество ошибок.

4. Чтобы преобразовать свои частично испорченные, и, возможно, не вполне секретные строки в пригодный к использованию ключ, Алисе и Бобу теперь нужна некоторая обработка. Основные шаги таковы: оценить уровень ошибок при передаче; сделать предположение о максимальном количестве информации, которая могла утечь из-за подслушивания; и затем скорректировать все ошибки, в то же время уменьшая количество информации, потенциально доступное Еве, до требуемого уровня. Оставшиеся биты и есть криптографический ключ.

Описанный протокол распределения квантового ключа называется BB84, его изобрели Чарльз Беннет и Жилль Брассард, соответственно, в 1984 году [3]. Протокол нашел свое первое практическое воплощение как раз с использованием поляризованных фотонов. Однако, использование именно этой схемы кодирования, поляризационной схемы, не очень удобно для передачи сигнала по оптоволоконным линиям связи – оно затруднено деполяризаций и флуктуациями двулучепреломления. Гораздо удобнее осуществлять распределение квантового ключа с использованием фазового кодирования.

2. Схема распределения квантового ключа на основе интерферометра Маха-Цандера.

В описанном выше поляризационном способе кодирования битов информации значение бита определяется поляризацией фотона: поляризован ли он по оси X или Y, ось Y повернута относительно оси X на $\pi/2$, и чтобы индетерминизм работал на нас, мы рассматриваем это в двух максимально ортогональных базисах, один из которых повернут относительно другого на $\pi/4$. С идейной точки зрения, фазовое кодирование аналогично поляризационному. Только рассматривается не поворот плоскости поляризации, а сдвиг импульса по фазе. Здесь тоже есть два базиса, но один из базисов сдвинут на $\pi/2$ относительно другого, а базисные оси отстоят друг от друга по фазе на π. В этой схеме оптический сигнал раскладывается на два импульса, которые потом сходятся вместе и интерферируют. Фазовое кодирование реализуется с использованием интерферометра Маха-Цандера, Рис. 2. И у Алисы и у Боба есть фазовый

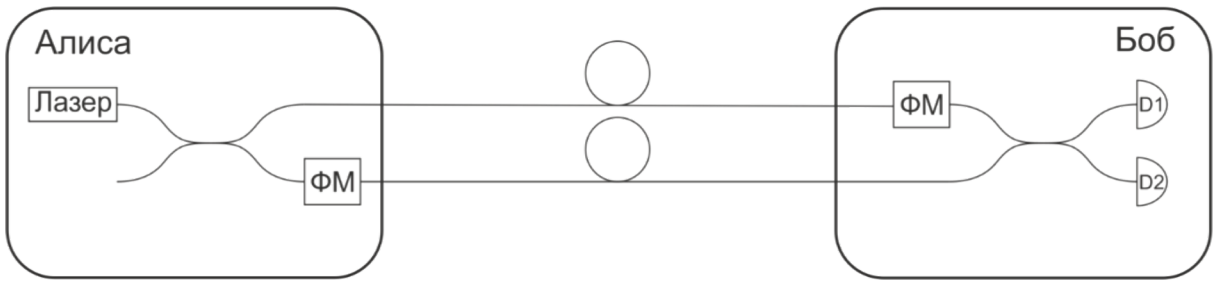


Рис. 2. Схема реализации фазового кодирования в интерферометре Маха-Цендера

модулятор. Алиса при помощи фазового модулятора создает разность фаз

между импульсами. Если разность фаз между импульсами равна 0, то на детекторе D1 создается конструктивная интерференция – интерференционный максимум, что соответствует значению бита 0. При этом на детекторе D2 реализуется интерференционный минимум – деструктивная интерференция. Если Алиса создает фазовый сдвиг равный π, то на детекторе D1 будет деструктивная интерференция, а на детекторе D2 – конструктивная, и это будет соответствовать значению бита 1. Т.е., в зависимости от сдвига фазы, у Боба будет срабатывать либо детектор D1, либо детектор D2, что будет означать либо получение бита 0 или 1.

Теперь надо добавить еще один базис, чтобы сделать передачу ключа секретной. Это обеспечивается введением со стороны Алисы еще двух фазовых сдвигов: π/2 и 3π/2. Получается, что фазовые сдвиги 0 и π соответствуют одному базису, для определенности, базису ⊕, а сдвиги π/2 и 3π/2 соответствуют базису ⊗. Боб, в свою очередь, может решать в каком базисе проводить измерения. Если определять интерференцию импульсов как они пришли, то это будет измерение в базисе ⊕, а если сдвинуть по фазе один из импульсов на π/2, то это будет измерение в базисе ⊗. Разумеется, и Боб и Алиса выбирают базис измерения и базис приготовления совершенно случайно. Таким образом, сохраняется вся последовательность действий протокола BB84, приведенная в Таблица *1*

3. Двухпроходная автокомпенсационная схема Plug&Play.

На Рис. 3 изображена оптическая схема Plug&Play, наиболее удобная с точки зрения простоты настройки параметров для распределения квантового ключа. Рассмотрим последовательность событий, происходящих с оптическими импульсами при квантовом распределении ключа в схеме Plug&Play.

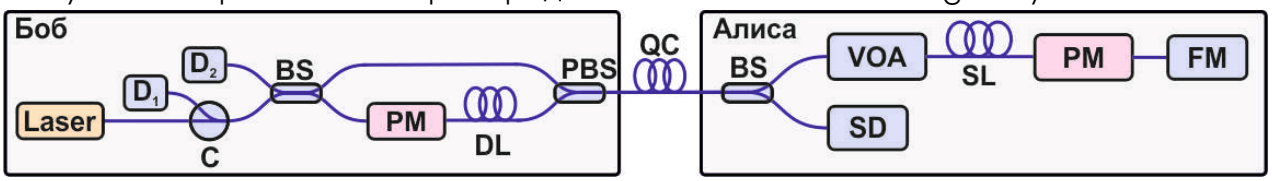


Рис. 3 Автокомпенсационная двухпроходная схема квантового распределения ключа "Plug&play". C – циркулятор, D1 и D2 – детекторы одиночных фотонов, PM – фазовые модуляторы, DL – линия задержки, PBS – поляризационный светоделитель, VOA – переменный оптический аттенюатор, SL – накопительная линия, FM – зеркало Фарадея.

1. Лазерный модуль, расположенный в блоке Боба, генерирует последовательность одинаковых многофотонных оптических импульсов, которую мы будем называть трейном. В нашем случае длина волны оптических импульсов λ = 1550 нм, импульсы линейно поляризованы. Частота следования лазерных импульсов – это одна из основных характеристик квантового распределения ключа. Обозначим эту величину как ν_0, соответствующий ей период – T_0, эти промежутки времени мы будем называть тактами. В трейне *n* импульсов и трейны следуют с периодом T_t – период трейна. Всего за сеанс формируется пакет из *N* трейнов. Промежуток между трейнами такой, что трейн успевает пройти расстояние от Боба до Алисы и обратно, и только после этого запускается

следующий. О факторах, ограничивающих в данной оптической схеме частоту ν_0 и количество импульсов в трейне, будет сказано ниже.

2. Блок Боба собран из волокна сохраняющего поляризацию (PM-волокно). Трейн лазерных импульсов попадает на циркулятор, который направляет лазерное излучение на светоделитель. В результате прохождения светоделителя каждый импульс разделяется пополам и направляется в соответствующие плечи интерферометра.

3. В одном из плечей интерферометра расположена линия задержки (DL) и фазовый модулятор, поэтому на поляризационный светоделитель импульсы, прошедшие через это плечо, приходят позже, следовательно, на выходе из поляризационного светоделителя получается в 2 раза больше импульсов, чем в первоначальном трейне. Время запаздывания описывается формулой:

$$t_{DL} = \frac{n_0 \cdot \Delta l}{c_0}, \tag{2}$$

где –длина линии задержки $n_0 \approx 1.47$ коэффициент преломления, c_0 – скорость света. На практике удобно использовать вытекающее из этой формулы соотношение: за 5 нс световой импульс проходит 1 м оптоволокна, т.е. получается, что скорость света в оптоволокне примерно равна 2×10^8 м/с. Из-за описанного смещения импульсы удобно рассматривать парами. Импульсы, преодолевшие большее плечо, имеют меньшую интенсивность из-за потерь, возникающих в линии задержки и фазовом модуляторе. Отметим, что импульсы, выходящие из PBS Боба, линейно поляризованы, причем их поляризация попарно ортогональна. Дальше трейн покидает Боба и через квантовый канал (QC) направляется к Алисе. Фазовый модулятор в длинном плече интерферометра Боба при прохождении импульсов в сторону Алисы не задействуется.

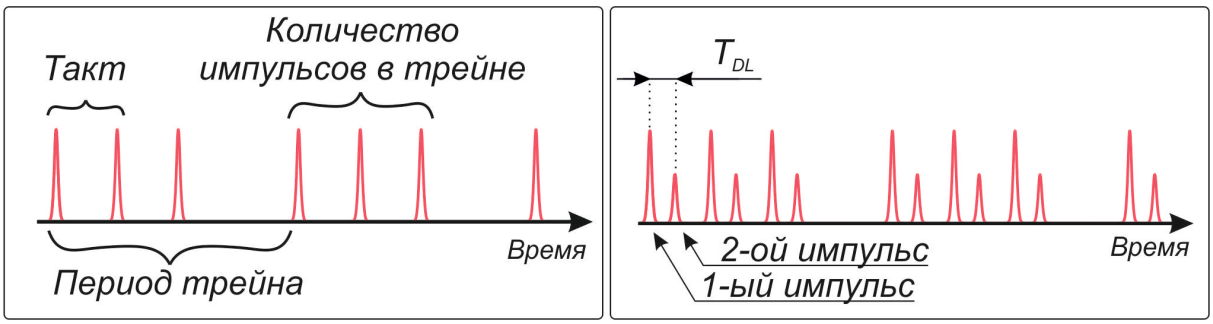


Рис. 4. Схема распространения импульсов на выходе из лазерного модуля и на выходе из поляризационного светоделителя

4. Приходя на оптическую схему Алисы, лазерные импульсы делятся на две неравные части: бóльшая часть оптической мощности идет на синхронизующий детектор SD, а меньшая часть используется дальше для обработки. Вся оптическая схема Алисы, как, впрочем, и QC, состоит из неподдерживающего поляризацию одномодового оптоволокна.

5. Синхродетектор SD служит для синхронизации всех быстрых процессов, в нашем случае - фазовой модуляции PM. Синхродетектор обозначает время прихода лазерных импульсов на оптическую схему Алисы. Теперь можно вовремя подать электрические сигналы на фазовый и амплитудный модуляторы Алисы, но с соответствующей задержкой.

6. До фазового модулятора Алисы импульсы еще должны пройти накопительную линию SL. Накопительная линия служит для того, чтобы вместить в себя все импульсы трейна. Собственно, длина накопительной линии и определяет количество импульсов в трейне, поэтому накопительная линия длинная – десятки километров. При движении трейна от Боба к Алисе неизбежно возникают множественные отражения на оптических неоднородностях, в основном на оптических разъемах. Эти отражения идут обратно к Бобу, и могут вызвать ложные срабатывания детекторов, информативным же является только сигнал, полученный при отражении трейна от зеркала Фарадея. Следовательно, для защиты от ложных срабатываний необходимо разделить по времени паразитные отражения и отражение от зеркала Фарадея, при этом не должно быть наложения, например, отражений от хвостовых импульсов трейна и уже возвращающихся обратно головных импульсов трейна. Для этого и служит накопительная линия, причем трейн может быть до 2 раз длиннее накопительной линии:

$$n \cdot T_0 \le 2\frac{n_0 \cdot L_{SL}}{c_0} \qquad (3)$$

здесь L_{SL} – длина накопительной линии. При расчете количества импульсов в трейне необходимо округлять значения в меньшую сторону до пяти сотен. Период трейна ограничен снизу длиной квантового канала + накопительная линия. Это ограничение накладывается по той же причине: не должно быть наложения импульсов идущих туда и обратно. Т.е. необходимо дождаться последнего импульса в трейне и только потом посылать новый. При расчете периода трейна необходимо округлять значения в большую сторону до пяти сотен.

7. Между накопительной линией и зеркалом Фарадея на один из импульсов каждой пары накладывается фазовый сдвиг фазовым модулятором Алисы, далее отраженные зеркалом Фарадея импульсы возвращаются обратно в накопительную линию. Отражаясь от зеркала Фарадея, лазерный импульс меняет свою поляризацию на ортогональную. Следует отметить, что фазовый сдвиг необходимо накладывать только на один импульс в паре, но при этом этот сдвиг должен накладываться на пути следования и туда, и обратно. Это диктуется особенностями работы фазового модулятора: дело в том, что фазовый модулятор сдвигает только одну компоненту поляризации, а направление поляризации у лазерных импульсов может быть непредсказуемым, поскольку они прошли по квантовому каналу, претерпели различные поляризационные искажения, и не известно под каким углом поляризации заходят в фазовый модулятор. Но после отражения от зеркала Фарадея поляризация меняется на ортогональную, и если

фазовый модулятор сдвинул одну компоненту поляризации в своем базисе, то на обратном пути он сдвинет как раз другую компоненту. Эти обстоятельства диктуют следующее ограничение: между входом фазового модулятора и зеркалом Фарадея должен находиться только один импульс из пары. Таким образом, получается, что время прохода импульсом расстояния от входа фазового модулятора и обратно не должно превышать времени между оптическими импульсами в паре. Если, к примеру, период следования лазерных импульсов T_0 =100 нс, и при этом после прохождения большего плеча интерферометра Боба второй импульс сдвигается на полпериода, то длина оптоволокна между фазовым модулятором и зеркалом Фарадея не должна превышать 5 метров.

8. От Алисы трейн импульсов направляется по квантовому каналу к Бобу. При этом поляризационные искажения и флуктуации двулучепреломления, которые трейн испытывал по пути к Алисе, компенсируются. В этом заключается преимущество схемы Plug&Play – нет необходимости в постоянной подстройке оптической схемы для компенсации искажений. Но у этой схемы есть и недостатки, например, из-за необходимости проводить передачу трейнами, существенно падает скорость распределения ключа.

9. Поскольку импульсы в трейне, будучи взаимно попарно ортогонально поляризованными, изменили свою поляризацию на противоположную при отражении от зеркала Фарадея, то теперь они проходят каждый по другому плечу интерферометра Боба. Поляризационный светоделитель направляет импульс в длинное плечо, если до этого он прошел по короткому плечу, и наоборот. Если оба фазовых модулятора – Алисы и Боба – не прикладывают сдвига, то на D2 реализуется конструктивная интерференция, а на D1 – деструктивная. Два базиса обеспечивают секретность передачи ключа. Алиса при помощи фазового модулятора прикладывает четыре фазовых сдвига: 0, $\pi/2$, π и $3\pi/2$. Получается, что фазовые сдвиги 0 и π соответствуют одному базису, например $\oplus$, а сдвиги $\pi/2$ и $3\pi/2$ соответствуют базису $\otimes$. Боб решает в каком базисе проводить измерения, либо не сдвигая фазу (базис $\oplus$), либо сдвигая фазу на $\pi/2$, то это будет измерение в базисе $\otimes$. И Боб и Алиса выбирают базис измерения и базис подготовки совершенно случайно.

4. Ослабление лазерных импульсов

Квантовое распределение ключа, основанное на протоколе BB84, требует, чтобы оптические импульсы были однофотонными. Если импульсы содержат больше одного фотона, то Ева может проводить атаку разделением числа фотонов и ключ будет скомпрометирован. Из-за сложности создания эффективного источника единичных фотонов, в реальных условиях квантовые состояния не являются однофотонными. Вместо однофотонных состояний на практике используются ослабленные лазерные импульсы, т.е. когерентные состояния со средним числом фотонов μ = 0.1-0.5 фотона/импульс. При малой

интенсивности распределение числа фотонов в импульсе подчиняется статистике Пуассона:

$$\mathrm{P}(n_p, \mu) = \frac{\mu^{n_p}}{n_p!} \exp(-\mu), \tag{4}$$

где n_p – число фотонов в импульсе. На Рис. *4* приведено распределение числа фотонов для разных значений μ.

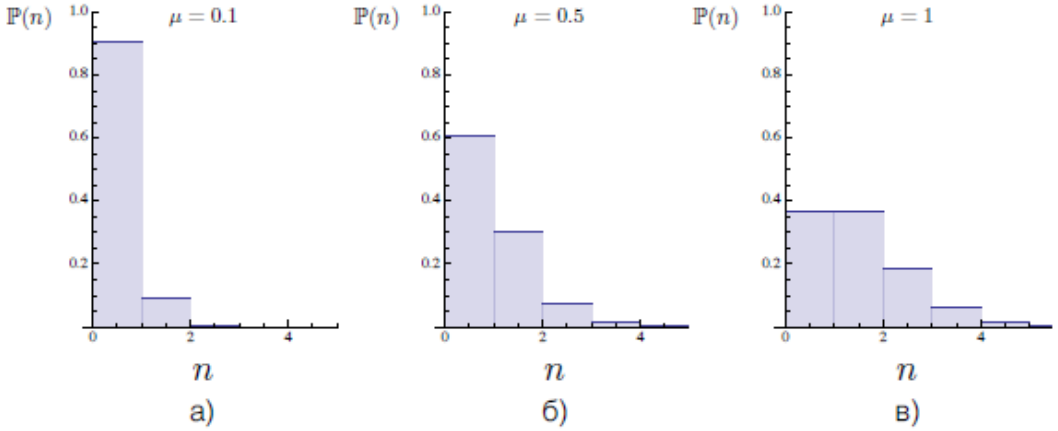


Рис. 4 Статистика Пуассона лазерного излучения: зависимость вероятности числа фотонов n в импульсе интенсивностью μ для (а) μ = 0.1, (б) μ = 0.5 и (в) μ = 1.0.

На рисунке видно, что если у нас в среднем 1 фотон на импульс, то около 37% импульсов у нас не содержат ни одного фотона, столько же по одному фотону, без малого 20% - 2 фотона, более 5% - 3 фотона, и даже у четырёх фотонных импульсов очень заметен вклад. Такое положение вещей совершенно неприемлемо – слишком много импульсов, на которых можно провести атаку расщеплением числа фотонов. Если же использовать импульсы с μ = 0.1, то как видно из графика, число импульсов содержащих 2 фотона и больше пренебрежимо мало. Правда за это приходится платить тем, что более 90% импульсов не содержат ни одного фотона вообще, из-за чего скорость распределения ключа сильно падает.

Лазерные импульсы необходимой мощности получаются при помощи аттенюатора VOA, который ослабляет трейн два раза: на пути туда и обратно. Для того, чтобы установить необходимое ослабление на аттенюаторе, например такое, что бы от Алисы выходили импульсы в среднем, скажем, 0.1 фотона/импульс, необходимо с помощью измерителя мощности определить мощность лазерных импульсов, выходящих из светоделителя Алисы. Но это измерение осложнено тем, что импульсы изначально слабые, а нам нужны еще сильнее ослабленные импульсы и все это выходит за пределы измерений измерителя мощности. Поэтому надо померить более мощные импульсы, а затем дополнительно ослабить мощность в нужное число раз. Лазерный модуль подключен к циркулятору через аттенюатор (или серию аттенюаторов). Это

сделано для того, чтобы не слепить D1 мощным светом, это может даже вывести его из строя. Можно предложить следующую последовательность действий:

1. Обязательно отключить оба детектора одиночных фотонов, чтобы не вывести их из строя. Для надежности лучше отсоединить оптические разъемы.
2. Используя источник непрерывного лазерного излучения измерить коэффициенты затухания в оптических схемах Боба и Алисы. Для расчета коэффициента затухания в оптической схеме используется формула:

$$\alpha_{att} = 10\lg\left(\frac{P_{in}}{P_{out}}\right), \tag{5}$$

где P_{in} – мощность излучения, входящего в оптическую схему, P_{out} – мощность излучения на выходе.

3. Из-за того, что между светоделителем и аттенюатором Алисы есть несколько оптических соединений, часть мощности отражается от этих разъемов. Поскольку после ослабления импульсов на VOA вышедший трейн очень слабый, вклад отраженного сигнала становится существенным, и при расчете коэффициента ослабления, необходимого для достижения требуемого числа фотонов на импульс, придется учесть коэффициент отражения на данном участке. Для определения коэффициента отражения на VOA выставляется большое значение ослабления (60 дБ), чтобы ничего не вышло наружу, и измеряется мощность отраженного сигнала P_r. Потом выставляется минимальное ослабление на VOA и тоже измеряется выходная мощность P_{out}. Пусть приходящая на VOA мощность P_{in}, тогда выходящая $P_{out} = P_r + P_{in}10^{-0.1\cdot 2\cdot(\alpha_v+\alpha_c)}$, где множитель 2 учитывает проход туда-обратно, α_c -неизменное ослабление канала, α_v - некоторое значение аттенюации на EXFO.
4. Мощность при которой в импульсе содержится необходимое нам среднее число фотонов μ, рассчитывается по формуле

$$P_0 = \frac{c_0 \nu_0 h \mu}{\lambda}, \tag{6}$$

где λ - длина волны лазерного излучения, в нашем случае λ = 1550 нм.

После проделанных измерений необходимо отсоединить оптоволокно лазерного модуля и подключить его к оптической схеме через аттенюатор. Только после этого можно подключить детекторы одиночных фотонов D1 и D2.

5 Практическая реализация схемы распределения квантового ключа

Основная проблема изготовления и настройки устройства квантовой криптографии – синхронизация всех оптических и электрических импульсов в устройстве. На Рис. 5 показана функциональная схема устройства, реализованная на базе FPGA плат National Instruments, программируемых на

LabVIEW. Кроме оптической схемы на этом рисунке показаны электронные

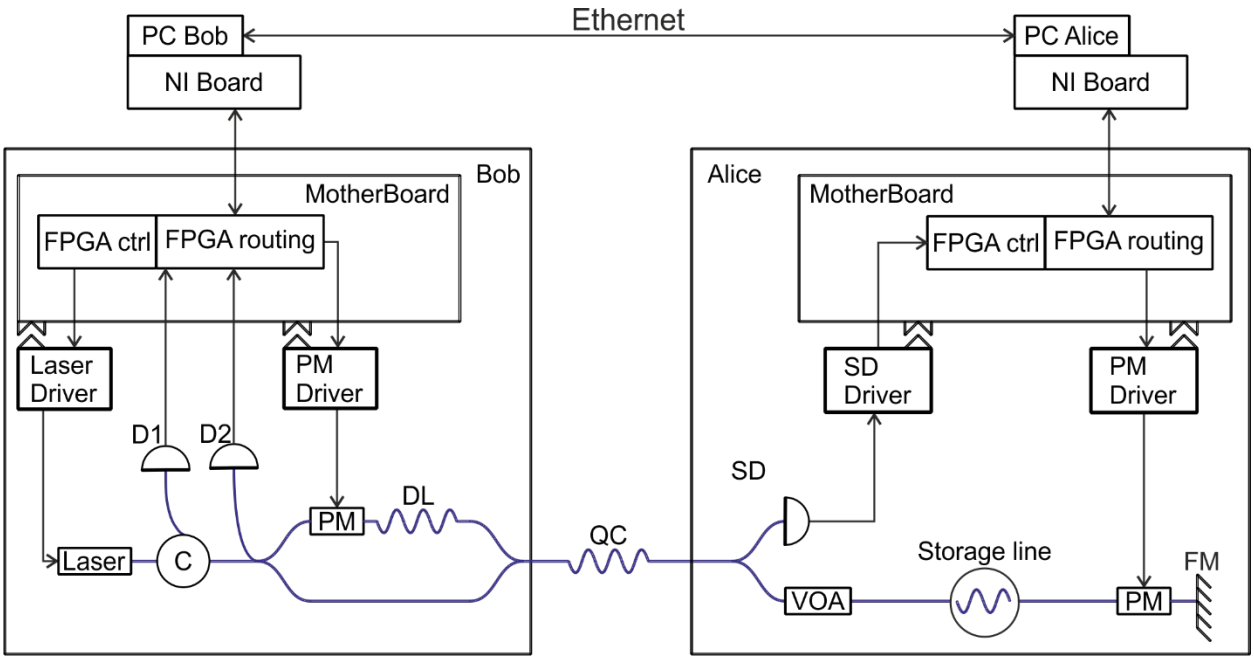


Рис. 5 Функциональная схема устройства квантовой криптографии. C – циркулятор, D1 и D2 – детекторы одиночных фотонов, PM – фазовые модуляторы, DL – линия задержки, PBS – поляризационный светоделитель, VOA – переменный оптический аттенюатор, SL – накопительная линия, FM – зеркало Фарадея.

модули и обозначены взаимодействия.

Лазерный драйвер (Laser Driver), драйверы фазового модуляторы изготовлены в виде небольших плат расширения. Эти платы можно вставлять в материнскую плату, которая по своей архитектуре идентичная и у Алисы и у Боба. Основная задача материнской платы – обеспечение связи между подключаемыми платами расширения и платой NI, установленной в обычном персональном компьютере. Плата NI соединяется с материнской платой с помощью PCI-кабелей. Кроме того, материнская плата осуществляет контроль за током питания плат расширения, в блоке Алисы выполняет задержку электрических импульсов, чтобы обеспечить их приход к оптическим модуляторам в нужное время, а в блоке Боба укорачивает до нескольких наносекунд электрический импульс, посылаемый на драйвер лазера.

Программное обеспечение, которое управляет системой распределения квантового ключа, было написано в среде разработки LabVIEW, продукта компании National Instruments. Это популярное средство, используемое учеными и инженерами, главным образом для сбора данных, управления оборудованием и промышленной автоматизации. Мы считаем LabVIEW приемлемым решением для образовательных целей. Данный продукт уже широко используется в университетском практикуме по физике, он будет знаком многим студентам. В то же время, те, у кого нет опыта работы с LabVIEW, легко могут включиться в

использование этой среды, поскольку язык программирования в ней графический и интуитивно понятный. Впрочем, для настройки установки и запуска генерации квантового ключа знание LabVIEW не требуется. Единственно, что необходимо знать – как запускать нужные для работы программы. Программное обеспечение, как Алисы, так и Боба состоит из двух уровней. Нижний уровень работает на FPGA платы NI, это программы, для работы которых требуется точная временная шкала. Эти программы посылают импульсы на лазерный драйвер, драйверы модуляторов, проверяют в нужное временное окно срабатывание детекторов одиночных фотонов. Программы этого уровня называют прошивкой или FPGA программой, или иногда целевой (target) программой.

Программа верхнего уровня работает на PC, она запускает программу нижнего уровня, принимает от нее данные, занимается просеиванием ключа. Эту программу называют хостовой (host). Если открыть проект LabVIEW, то для доступа к целевым программам необходимо раскрыть ветку FPGA Target, Рис. 6. Хостовые программы расположены на уровень выше. Для настройки установки и запуска

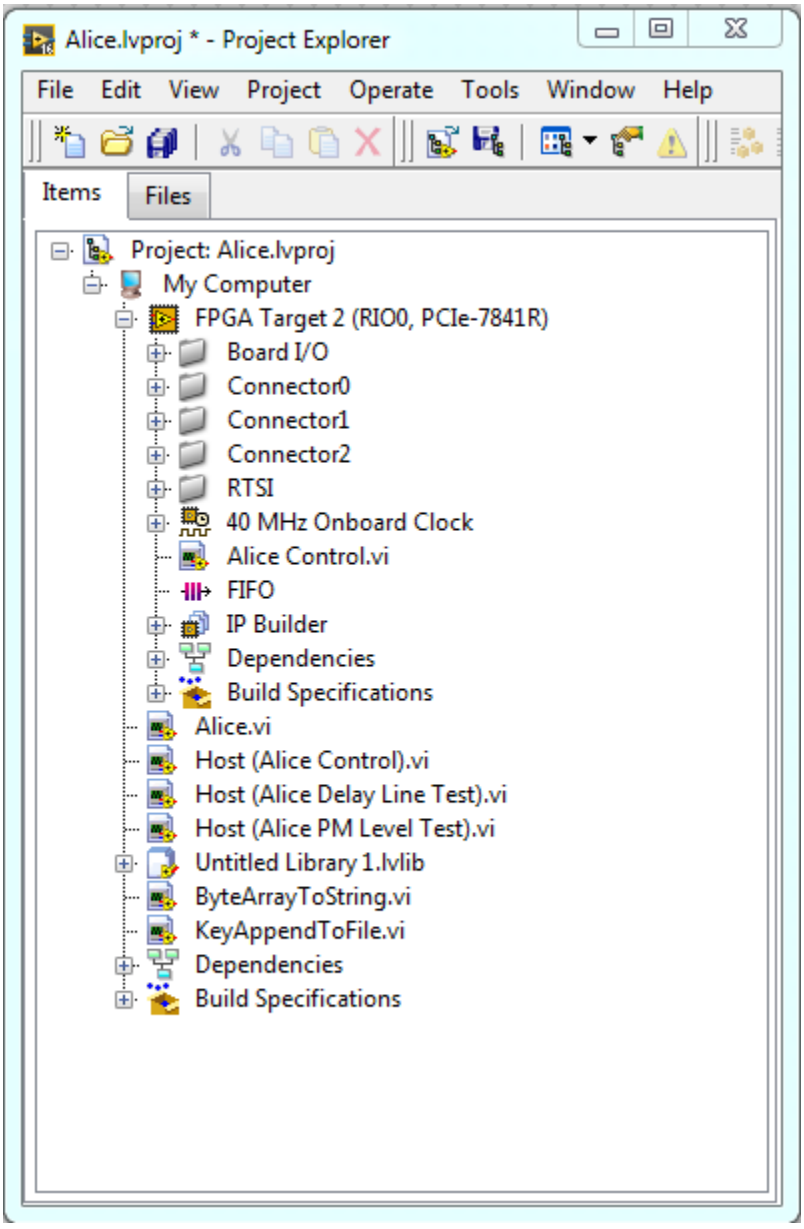


Рис. 6. Пример окна проекта LabVIEW

генерации квантового ключа нужны только программы хостового уровня. Программы имеют расширение vi.

Для запуска какой-либо программы нужно дважды кликнуть по ее названию. После этого откроется окно самой программы. В этом окне по необходимости надо скорректировать рабочие параметры, а затем запустить программу на выполнение, кликнув по стрелке, Рис. 7. Для остановки программы надо нажать на

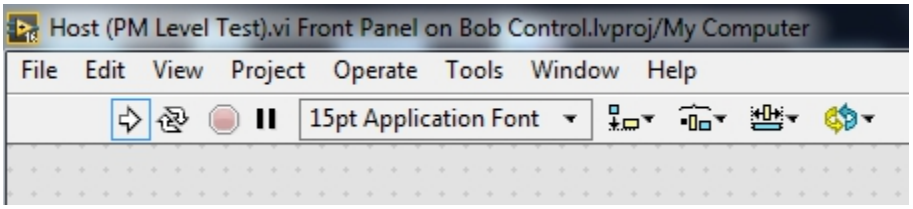


Рис. 7. Изображение окна запуска проекта LabVIEW

знак «Стоп», правее стрелки, который во время работы программы становится активным и красным.

6. Процедуры настройки устройства квантовой криптографии

Квантовое распределение ключа требует точной синхронизации оптических и электрических импульсов во всей схеме Plug&Play. Это приводит к необходимости предварительной настройки всей схемы. Также через некоторое время возможно возникновение необходимости корректировки настроечных параметров, например, из-за изменения длины оптоволоконных каналов при колебаниях температуры. В этом разделе перечислены основные настроечные процедуры, которые необходимо проделать, прежде чем удастся получить ключ. Также описывается графический интерфейс программных приложений и, поскольку он может меняться, описывается сама идея настройки криптографического устройства.

6.1. Настройка времени ожидаемого прихода импульсов на детекторы Боба.

Как уже говорилось, при движении оптических импульсов от Боба к Алисе возникают множественные отражения, которые вызывают срабатывания детекторов Боба. Разумным представляется регистрировать срабатывания детекторов одиночных фотонов только в те временные окна, когда ожидается приход импульсов от Алисы. Программа Host (Channel Test).vi расположена в прошивке Боба и служит для определения номера такта, в который импульс возвращается к Бобу. Номера тактов отсчитываются от момента отправления трейна на Алису.

Channel Test работает следующим образом. От Боба выходят одноимпульсные трейны, после прохождения оптических схем Боба и Алисы, они регистрируется детекторами одиночных фотонов (ДОФ). Набирается статистика срабатывания ДОФ по номерам тактов и по полученным данным строится гистограмма (рис. 9), где по оси x отложены номера тактов, а по оси y – количество срабатываний детектора. Последний импульс на гистограмме

соответствует отражению от крайнего элемента в оптической цепи – от зеркала Фарадея.

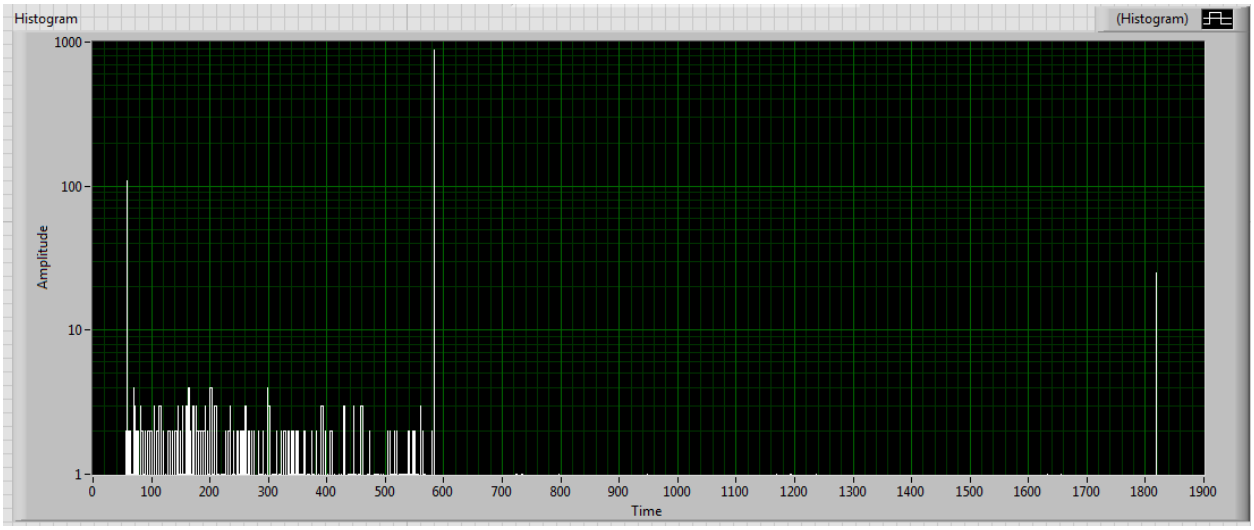


Рис. 9. Гистограмма срабатывания ДОФ

Такт прихода именно этого импульса необходимо использовать для открытия окна регистрации сигнала детектором. На рис. 10 показана гистограмма с увеличенным масштабом по оси x построенная для трейнов с пятью импульсами.

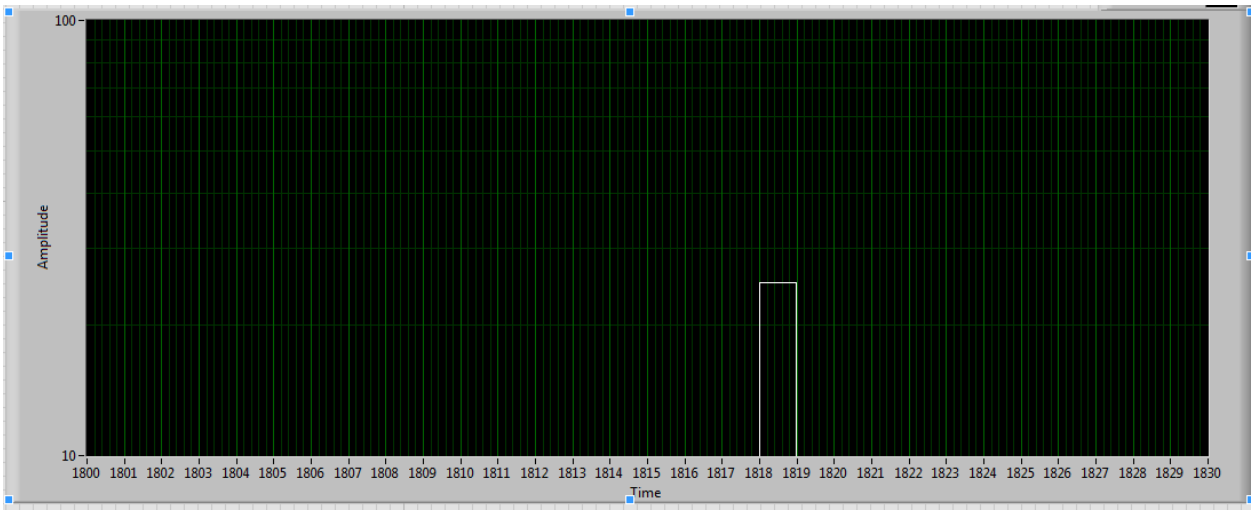


Рис. 10. Гистограмма срабатывания ДОФ с увеличенным изображением сигнала, полученного при отражении от зеркала Фарадея

В программных интерфейсах найденное значение будет соответствовать открытию большого окна для ДОФ-ов, и называется этот параметр Open Window. Для случая, изображенного на гистограмме, искомое число будет равно 1818, оно определяется по времени прихода первого импульса в нашем пяти импульсном трейне. Импульсы на гистограмме могут удваиваться, это происходит потому, что регистрация счета детекторов одиночных фотонов происходит в более мелкие временные окна, чем отображает шкала гистограммы, так что сигнал может быть

зарегистрирован в 2 разных окна. Соответствующий параметр нам еще предстоит настроить. Здесь же при нашей точности измерения оба парных импульса соответствуют одному лазерному импульсу. Для подтверждения правильности выбранного рефлекса можно провести следующие действия: изменить напряжение на фазовом детекторе (DAC Level), изменить количество импульсов в трейне, при этом должно увеличиться количество рефлексов, а удостовериться, что номер такта определен правильно можно изменяя отрываемое окно. Полученный номер такта следует выставлять во всех последующих подпрограммах в поле открытия временного окна (Open Window). Закрывается временное окно после прихода последнего импульса в трейне, т.е. в поле Close Window надо выставить число, полученное суммированием количества импульсов в трейне с Open Window.

6.2 Настройка напряжения на фазомодуляторах Боба и Алисы.

Подпрограмма Боба Host (Mod Level Test).vi находится в прошивке Боба и служит для нахождения величины напряжения, которое надо подавать на фазовый модулятор для сдвига оптического импульса на фазу π. При запуске программы происходит отправление серии трейнов, содержащих 10-30 импульсов, в то время как напряжение, подаваемое всякий раз на фазовый модулятор изменяется на небольшую величину (DAC interval). Если на некотором ДОФ-е при отсутствии напряжения на модуляторах реализовывался интерференционный минимум, то постепенно увеличивая на одном из модуляторов напряжение, должен реализоваться максимум. На рис 11 ось x представлена в относительных единицах, определяемых разрядностью цифро-аналогового преобразователя драйвера фазового модулятора. По оси y – количество срабатываний ДОФ-а.

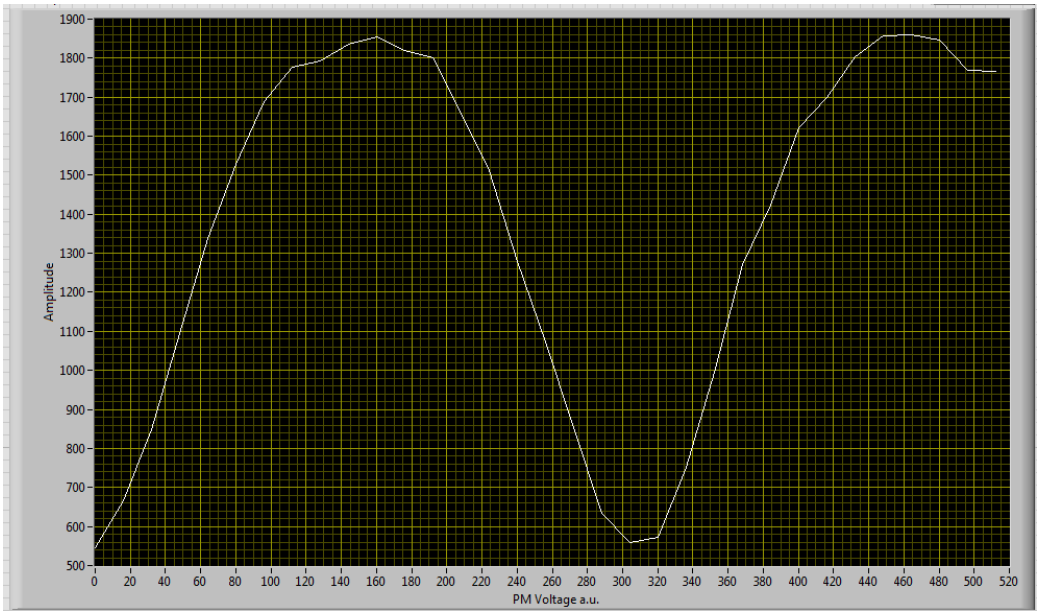


Рис. 11. График зависимости амплитуды сигнала от напряжения, поданного на фазовый модулятор

Видно, что для данного графика максимум, соответствующий координате середины полуширины кривой, находится примерно на 160 отн.ед. Для второго детектора такой же график должен проходить через минимум.
Процедура настройки напряжения соответствия сдвигу фазы на π проводится для фазовых модуляторов Алисы и Боба порознь. Для этого используются разные, но схожие в плане интерфейса подпрограммы. После этого в соответствующих полях программ Алисы и Боба для распределения ключа надо будет выставить полученные величины. Данное значение напряжения в условных единицах называется в других программах DAC Level, DAC – Digital-to-Analog Converter.

6.3 Настройка величины задержки приложения напряжения на фазовый модулятор Алисы.

Время прихода оптических импульсов регистрируется синхродетектором Алисы. Но до того, как импульс будет сдвинут на фазовом модуляторе, ему еще предстоит пройти накопительную линию и квантовый канал, затратив на это некоторое время. Для нахождения точного значения временной паузы, которую надо выдержать перед приложением напряжения на фазовый модулятор, надо запустить и на Алисе, и на Бобе одновременно одноименные программы Host (Alice Delay Line Test).vi. Интерфейс этих программ разный: программа Боба посылает лазерные импульсы и отсылает Алисе информацию о срабатывании детектора одиночных фотонов. Алиса изменяет с определенным шагом время задержки (SPI Interval) и строит график (рис.12).
Появление данного графика поясняет рис. 13. До тех пор, пока величина задержки недостаточна (задержка t_1), электрические импульсы, подаваемые на PM Алисы, опережают оптические и на D2 реализуется максимум, как и должно быть в отсутствие модуляции. По мере увеличения задержки, последний электрический импульс накрывает первый оптический, так что мы видим на графике первый минимум. Дальше мы продолжаем увеличивать время задержки, проходя через серию минимумов, до тех пор, пока вся электрическая последовательность импульсов не совместится с оптической. Это будет соответствовать искомой задержке, на графике примерно 24648. Горизонтальная шкала графика имеет размерность метр.

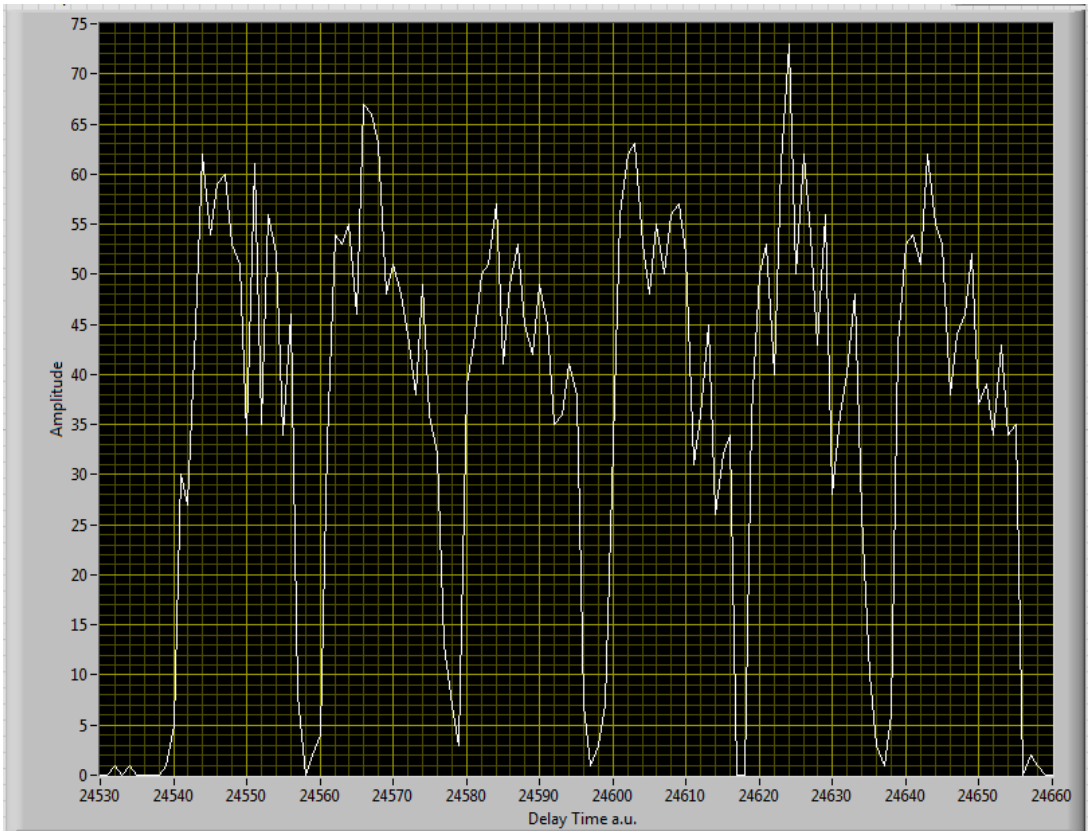


Рис. 12. График зависимости количества счета D2 (амплитуда сигнала, регистрируемого детектором) от времени задержки приложения напряжения на фазовый модулятор Алисы. *Этот график был получен при отправлении серий пяти импульсных трейнов (после прохождения разных плеч интерферометра Боба импульсы удваиваются). Время задержки откладывается по оси x*

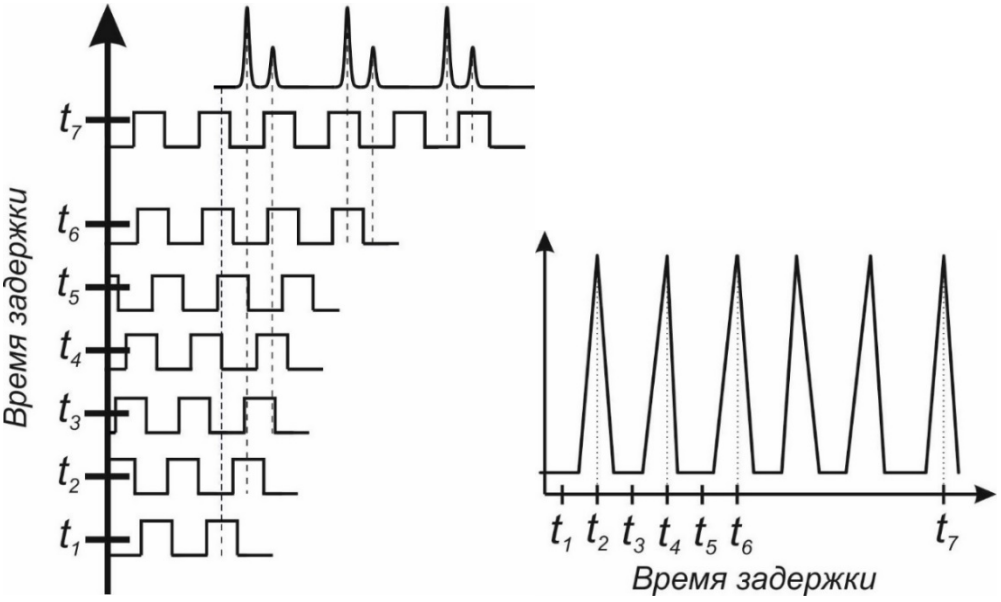


Рис. 13. Схема возникновения модуляции при изменении времени задержки подачи импульса на фазовый модулятор

Если для измерения использовать другой детектор – D1 –, то график будет инвертирован – минимумы и максимумы поменяются местами.

Для поиска величины задержки вначале надо оценить каким будет значение задержки, исходя из длины квантового канала и накопительной линии. Для работы необходимо открыть одно окно ожидания прихода импульса. Затем надо выбрать количество импульсов в трейне для изначального поиска этой величины. Разумно выбрать такое количество, что бы результат поиска был растянут на 1000 – 2000 единиц по шкале графика. Соответственно этим оценкам выставить начальную и конечную точку поиска – DL SPI (min) и DL SPI (max), их значения тоже измеряются в метрах. Здесь DL – Delay Line. Далее надо выбрать шаг поиска – Delay Line Delta. Единичный шаг поиска соответствует приращению величины задержки по цене делению, это может быть довольно долго. Поэтому, вначале надо выбрать достаточно большой шаг, но не кратный периоду следования импульсов. Таким образом, надо несколько раз повторить процедуру, всякий раз уменьшая шаг, количество импульсов, интервал сканирования, вплоть до точного нахождения величины задержки. Последнее измерение проделывается для 3-7 импульсов в трейне.

6.4 Точная настройка временных окон детекторов D1 и D2.

Как уже указывалось выше, временное окно величиной в такт – это довольно грубая величина. В целях уменьшения темнового счета, дающего основной вклад в QBER, разумно уменьшить временное окно регистрации пришедших сигналов для каждого детектора. В разработанном ПО для каждого детектора индивидуально настраивается временное окно шириной 10 нс. Для проведения этой настройки отправляются многоимпульсные трейны и собирается статистика для каждого из малых окон при помощи программы Боба Host (Window Test).vi, рис. 14. Для периода следования импульсов 200 нс у нас 40 окон – от 0 до 39.

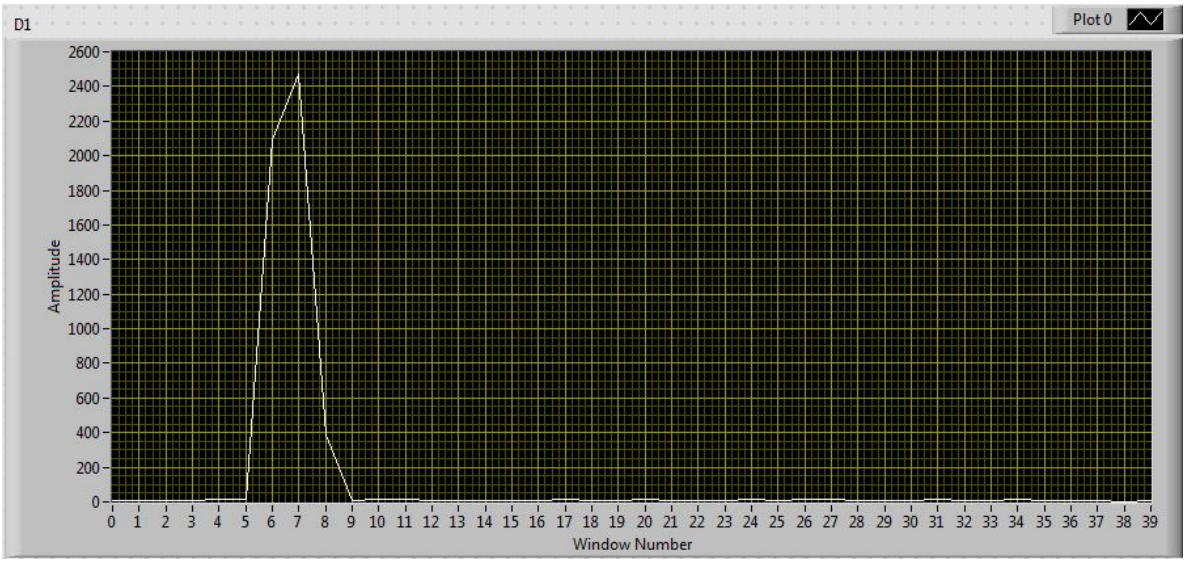


Рис. 14. График зависимости количества счета D2 от окна регистрации

На рисунке видно, что максимальный счет детектора соответствует 7-му окну, и он ненамного больше счета в 6-м окне. Значение настроечного параметра, задаваемого в программе Боба распределения квантового ключа – 7.

Данный параметр наиболее чувствителен к изменению внешних условий, так что надо иметь ввиду, что во время работы устройства и возможного нагрева/охлаждения квантового канала велика вероятность перехода регистрации измерений в соседний такт. Следует также отметить, что для нахождения номера окна для D1 надо выставлять сдвиговое напряжение, соответствующее сдвигу π на фазовом модуляторе Боба. Для нахождения номера окна для D2 наоборот, надо убедиться, что на фазомодулятор Боба не подается напряжения.

6.5 Настройка времени подачи сигнала на фазовый модулятор Алисы

Как было описано ранее, фазовый сдвиг необходимо накладывать только на один импульс в паре, но при этом этот сдвиг должен накладываться на пути следования и к зеркалу Фарадея и от него. Для настройки времени включения и выключения напряжения на фазовом модуляторе необходимо варьировать параметры в полях "PM Data on" и "PM Data off", где указывается количество тактов, отсчитываемых с момента прихода синхронизирующего сигнала.

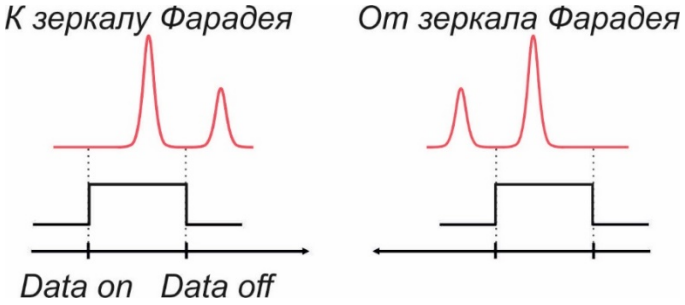


Рис. 15. Схема иллюстрирующая соотношение времени прихода электрического импульса на фазовый модулятор и оптического сигнала

Для контроля данных параметров необходимо подключиться щупами осциллографа к ножкам CLK данных ЦАП-а и, изменяя параметры полях "PM Data on" и "PM Data off", добиться оптимальной длительности импульса, подаваемого на фазовый модулятор (синий сигнал рис. 12).

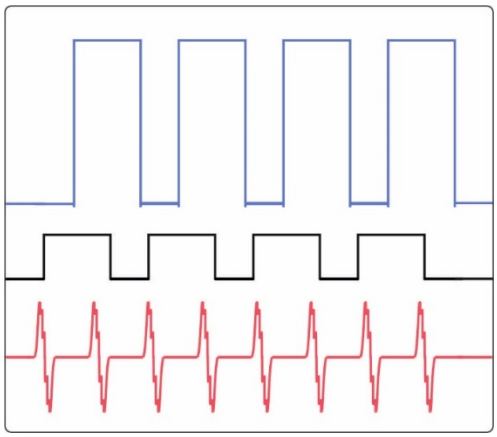


Рис. 16. Синий сигнал электрический импульс, поступающий на фазовый модулятор, черный-CLK, красный такты запуска

6.6 Возможность генерации квантового ключа с использованием одного детектора одиночных фотонов.

Протокол BB84 позволяет осуществлять квантовое распределение ключа с использованием только одного детектора одиночных фотонов. Для этого Бобу необходимо случайным образом выбирать не только базис измерения, но то, что он собирается проверить в данном базисе – «0» или «1». Если он угадал и с базисом и с битом, то детектор кликнет. Если не угадал с базисом, то детектор кликнет с вероятностью 50%. Если Боб угадал с базисом, но не угадал с битом, то детектор не кликнет, но такие случаи все равно будут выброшены. Данная логика приведена без учета того, что фотона может не быть, что детектор неидеален, конечно надо эти обстоятельства иметь в виду.

В нашем случае схемы "Plug and play" на фазовый модулятор Боба случайным образом подается не два значения напряжения, как в случае работы с одним ДОФ-ом, а также как и у Алисы четыре значения, соответствующих сдвигам по фазе 0, $\pi/2$, π и $3\pi/2$. Для тех событий, в которых Боб зафиксировал клик, он сообщает Алисе по открытому каналу базис измерения: базис I – это сдвиги 0 или π, базис II – сдвиги $\pi/2$ или $3\pi/2$. Информацию, какой бит проверялся в данном базисе Боб оставляет в секрете. После этого Алиса и Боб оставляют себе биты в совпадающих базисах и, таким образом, получают просеянный ключ. При распределении ключа с использованием одного ДОФ-а ключ получается, по крайней мере, в 2 раза короче, чем при использовании 2-х ДОФ-ов.

Процедуры настройки для работы с одним ДОФ-ом ничем принципиально не отличаются от таковых для двух ДОФ-ов. Принципиальное отличие – точная настройка временного окна проводится только для одного детектора, например, для D1. Для запуска генерации ключа как у Алисы, так и у Боба хостовая программа переводится в режим работы с одним детектором.

6.7. Запуск генерации ключа

Для запуска генерации ключа необходимо воспользоваться программами Боба и Алисы Bob Key Distribution.vi и Alice Key Distribution.vi. Для успешного запуска необходимо ввести ранее найденные параметры в рабочие окна программ. Если все параметры были найдены верно, то запустится передача ключа. При этом программа будет отображать длину ключа и величину ошибки (QBER). Смещая окна детекторов можно увеличить длину ключа, а изменяя время задержки, можно уменьшить величину QBER.

7. Параметры детектора одиночных фотонов

1. Квантовая эффективность (RF) — вероятность регистрации одиночного фотона, другими словами, отношение количества зарегистрированных фотонов к общему числу пришедших фотонов. Для целей квантовой криптографии значение этого параметра в идеале должно приближаться к единице.

Для определения квантовой эффективности детектора необходимо определить количество фотонов, которое посылается на детектор (*N*), а потом количество зарегистрированных детектором фотонов (*C*).

$$RF = \frac{C}{N}$$

Количество фотонов, выходящие из источника лазерного излучения можно определить, измерив мощность и воспользовавшись формулой (6):

Однако, для корректной работы ДОФ лазерные импульсы, поступающие на него, должны быть ослаблены настраиваемым аттенюатором. Следовательно, количество фотонов *N*, которые он зарегистрирует будет определяться формулой:

$$N = N_l 10^{-\frac{\alpha_{att}}{10}}, \quad (7)$$

где N_l – количество фотонов направленное в аттенюатор, a_{att} – коэффициент затухания в дБ.

Количество срабатываний ДОФ можно узнать, воспользовавшись рефлектограммой.

2. Частота темновых отсчетов (EDS) — количество ложных срабатываний детектора в единицу времени в отсутствие фотона. Данная величина является характеристикой собственных шумов детектора.

Количество ложных срабатываний детектора можно определить воспользовавшись частотомером, который показывает количество срабатываний за определенный промежуток времени. Для этого сигнал с детектора следует переключить на частотомер.

3. «Мертвое» время (DT) – время после зарегистрированного импульса, в течение которого невозможна регистрация следующего фотона. Данный параметр легко определить с помощью осциллографа рис. 17. На детектор подается серия импульсов, а сигнал с детектора направляется на осциллограф. В данном случае значение составило 8,8 мкс.

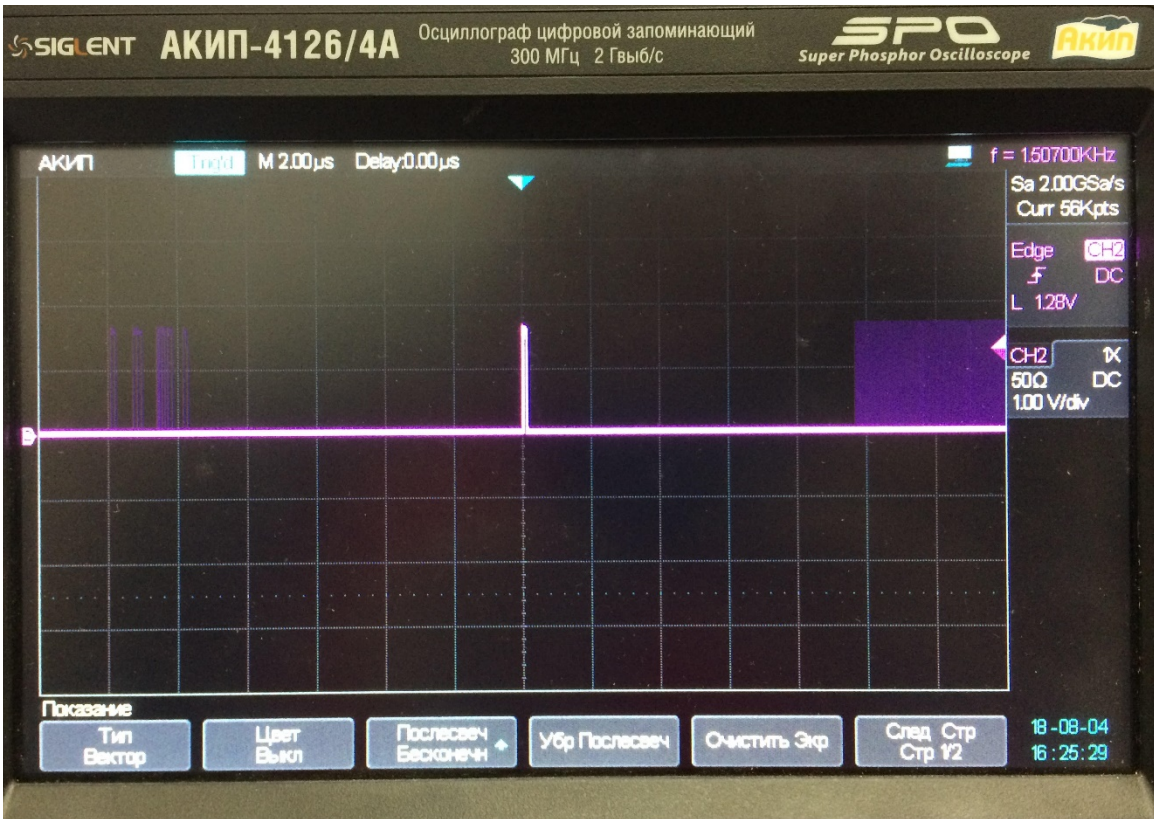


Рис. 17. Изображение экрана осциллографа при регистрации мертвого времени детектора

Сокращения и обозначения

QBER – Quantum Bir Error Rate

Train period – период следования трейна, измеряется в тактах следования лазерных импульсов

Open Window – такт на который открывается регистрация лазерных импульсов у Боба

Close Window – такт на который закрывается регистрация лазерных импульсов у Боба

DAC Level – сигнал на ЦАП драйвера фазомодулятора, соответствует амплитуде напряжения импульса, посылаемого на фазомодулятор Алисы или Боба, в относительных единицах

DAC Interval – шаг изменения DAC Level при сканировании

Time Sample – время измерения (набора статистики) одной точки графика, в миллисекундах.

DL SPI – величина задержки сигнала, подаваемого на фазомодулятор Алисы. В настоящее время измеряется в метрах, которые необходимо сигналу пройти по оптоволокну. SPI – это последовательный интерфейс, при помощи которого величина задержки посылается на ПЛИС, которая эту задержку осуществляет

SPI Interval – шаг изменения DL SPI при сканировании
Check D1 и Check D2 – маленькие окошки внутри большого окна (Window, которое измеряется в тактах) на которые включается регистрация фотонов ДОФ1 и ДОФ2. В настоящий момент большое окно делится на 40 маленьких.
Pi/2, Pi, 3Pi/2 Voltage – напряжение в относительных единицах, подаваемое на фазомодуляторы Боба и Алисы для смещения фазы на π/2, π и 3π/2. Смещение на π соответствует величине DAC Level, для подачи напряжения π/2 и 3π/2 надо домножить величину DAC Level на 1/2 и 3/2, соответственно.

Список литературы

1. Gisin N. et al. Quantum cryptography // Rev. Mod. Phys. 2002. Vol. 74. P. 145–195.
2. The Physics of Quantum Information: Quantum Cryptography, Quantum Teleportation, Quantum Computation / ed. Bouwmeester D., Ekert A.K., Zeilinger A. Springer, 2000. 315 p.
3. Bennett C.H., Brassard G. Quantum cryptography: Public key distribution and coin tossing // IEEE Int. Conf. on Comput. Sys. and Sign. Proces., Bangalore, India, December 1984. 1984. P. 175–179.